Trade Secret Management Guidelines

2010

営業秘密管理指針（改訂版）

| 経済産業省 知的財産政策室 |

Ⅰ．営業秘密管理とは

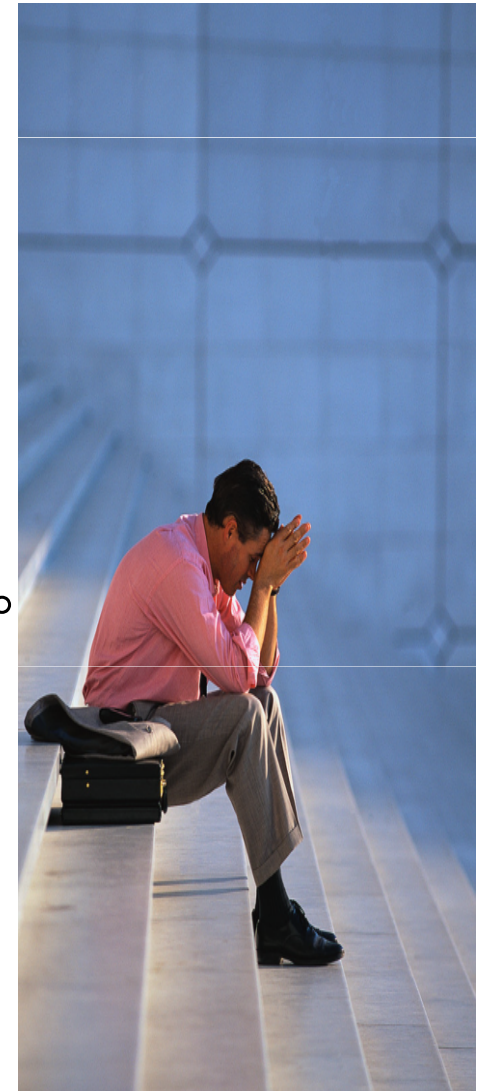
こんな事例耳にしたことありませんか？

○虎の子の重要な情報を適切に管理していなかった。

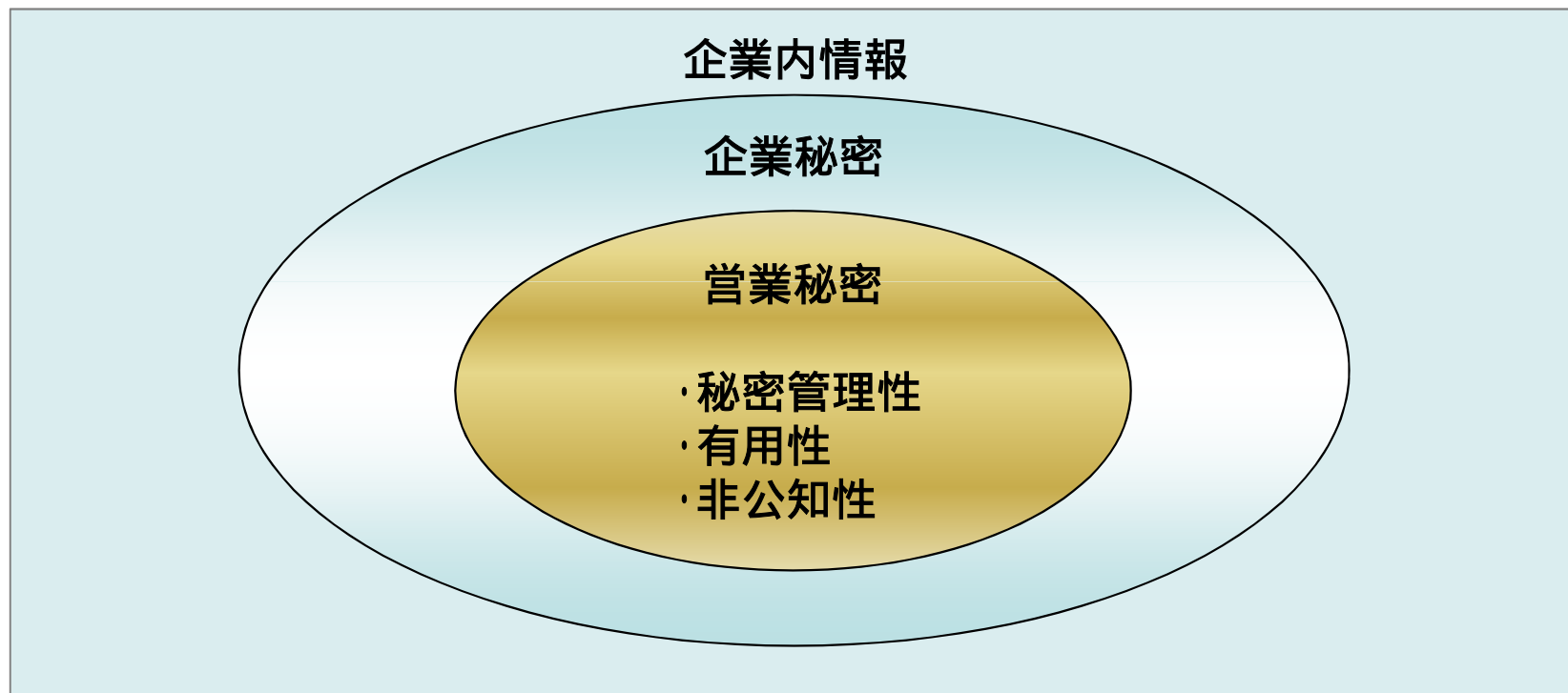
➢従業員が退職時に顧客名簿を持ち出してライバル会社に
転職した…
ライバル会社に有望な顧客を奪われてしまった。

➢仕入先リストが盗まれた…
製品の価格優位がなくなってしまった。

○虎の子の重要な情報を安易に公開してしまった。

➢開発中の製品の製造方法を特許出願したら、
出願公開制度を通じて一般の知るところとなった…
ライバル会社に周辺特許を取られてしまった。

営業秘密とは　（1）企業秘密との違い

○企業が秘密としている技術、ノウハウ、経営情報、顧客情報等は、「企業秘密」等といわれることがある。

○「営業秘密」は、このような「企業秘密」とされる情報と重なることが多いが、不正競争防止法上の要件（秘密管理性、有用性、非公知性）をすべて満たしたもののみが該当する。

営業秘密とは　(2) 裁判例において営業秘密として主張された情報

技術情報	製造方法（ノウハウ）	・製袋機の製造工程 ・白アリ防除剤製造方法（配合割合、加熱温度、攪拌方法・攪拌時間、冷却温度等） 等
	図　面	・金型図面 ・組立図面 ・部品図面 等
	そ　の　他	・ソフトウェアのプログラム ・機械効率のデータ 等
営業情報	経　営　情　報	・ソフトウェアの開発方針 ・取締役議事録 等
	仕入先／販売先に関する情報	・野菜の輸入先目録（生産者の氏名、住所、連絡先等） ・商品の原価 ・顧客目録（顧客の名称、住所、連絡先、過去の取引実績及び支払状況等） ・電話帳より抜粋した顧客名簿（ただし、電話勧誘の際の反応、成約に至る見込みなども記載） 等
	そ　の　他	・従業者（システムエンジニア）の情報（連絡先、売上高、報酬額、その差額である粗利益等） ・派遣会社における派遣社員情報（氏名、連絡先、年齢、性別、経歴、取得資格、派遣実績等） 等

営業秘密とは　(3) 営業秘密と特許権等との対比

	営業秘密として管理	特許権等の知的財産権を取得
メ リ ッ ト	•自社の事業戦略の方向性が他社に明らかとならない •失敗した実験のデータ等特許になじまないノウハウも営業秘密として保護対象となり得る •製品等を分解することによって明らかにならない限り、保護期間の制限もなく他社との差別化を図れる	•事前の審査を通じ権利の内容が明確となる •登録を通じ権利の存否が明確となる •一定期間、譲渡可能な排他的独占権を取得できる
デメリット	•登録制度がないので、権利の内容、存否が不明確 •他社が独自開発した場合、独占できなくなる •適切に管理しない場合、法律による保護を受けられない	•出願内容を公開することを制度の前提としており、自社の開発動向が知られたり、周辺特許を取得されたりする可能性がある •保護期間が満了したら誰でも利用可能となる

「営業秘密管理」の意義　（1）経営戦略の一環

○知識集約型経済の発展に伴い、無形資産である技術・ノウハウ・アイデア等の創出、管理、活用、結合等の重要性が高まっている。

○無形資産の中から営業秘密として管理すべき情報を把握することは、自社の強みを把握でき、それらを最大限に生かした経営戦略（知的資産経営）につながるため、営業秘密管理は経営戦略の一部として行うことが重要。

「営業秘密管理」の意義　(2) 知財戦略の選択肢のひとつ

〇技術・ノウハウ等を活用して、利益を持続的に確保するには、他社に「使用させる部分」と「使用させない部分」とを明確にする必要がある。

〇そして、それぞれの部分について特許等を用いた「オープン化」と営業秘密として管理する「ブラックボックス化」とを戦略的に使い分けることが求められる。

※こうした使い分けは、今後、大企業のみならず、中小企業においても求められるものと考えられる。

技術・ノウハウ等を保護するには

公開（オープン化）して権利取得

- 特許権
  - 〇発明を保護
  - 〇原則出願から２０年

非公開に（ブラックボックス化）して保護

- 営業秘密
  - 〇保護期間に制限なし

各企業においてベストミックスを追求

Ⅱ．営業秘密管理指針について

営業秘密管理指針とは

〇適切な営業秘密管理に向けた企業のアプローチを支援することを目的に策定されたガイドライン。

〇「営業秘密」として法的に認められうる秘密管理の水準を示している。

営業秘密管理指針

平成１５年１月３０日
平成１７年１０月１２日改訂
平成２２年４月９日改訂

経済産業省

営業秘密保護に係る制度整備及び管理指針策定・改訂の経緯

平成２年　民事保護規定の創設

「営業秘密」の不正取得・使用・開示行為に対する民事保護規定の創設

平成14年　「知的財産戦略大綱」

企業が営業秘密に関する管理強化のための戦略的なプログラムを策定できるよう、「参考となるべき指針」を2002年度中に作成することが盛り込まれる

平成15年　「営業秘密管理指針」の策定・公表

平成15年　「営業秘密侵害罪」の創設

営業秘密侵害行為のうち、特に違法性の高い行為類型に限定して刑事罰の対象とする

平成16年　裁判所法等の改正

民事訴訟における営業秘密保護のための秘密保持命令制度、当事者尋問等の公開停止規定導入

平成17年　「営業秘密侵害罪」の罰則強化

国外処罰規定、退職者処罰規定、法人処罰規定等の導入（平成17年11月1日施行）

平成17年　「営業秘密管理指針」の改訂・公表

平成18年　「営業秘密侵害罪」の罰則強化

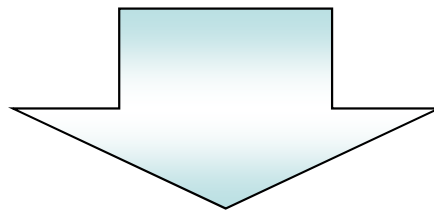
懲役刑の上限を１０年、罰金刑の上限を１０００万円、法人重課の上限を３億円に引き上げ（平成19年1月1日施行）

平成21年　「営業秘密侵害罪」の罰則強化

目的要件の変更、第三者等による営業秘密の不正な取得に対する刑事罰の対象範囲の拡大、従業者等による営業秘密の領得自体への刑事罰の導入（平成22年7月１日施行）

平成22年　「営業秘密管理指針」の改訂・公表

平成２１年不競法改正時の指摘とそれを踏まえた指針の改訂点

① 処罰対象となる行為、ならない行為を具体的に明らかにするべきではないか。
② 高度な管理水準を一律的に要求しているような印象を与えているのではないか。
③ 中小企業等にとって、より使いやすいものにするべきではないか。

① 処罰対象行為の明確化 →第２章
② 合理性のある秘密管理方法の提示 →第３章
③ 中小企業向けの参照ツールなどの提示 →参考資料

第１章　概説
第２章　不正競争防止法上の営業秘密の保護
第３章　営業秘密を保護するための管理の在り方

参考資料１　営業秘密管理チェックシート
参考資料２　各種契約書等の参考例
参考資料３　我が国における情報管理に関する各種ガイドライン等について
参考資料４　営業秘密を適切に管理するための導入手順について
～はじめて営業秘密を管理する事業者のために～

Ⅲ．営業秘密管理指針（改訂版）の内容

○知的資産経営
競争力の維持・強化の観点から、事業者が無形の経営資源である技術・ノウハウ等を強みとして把握し、これらを適切に管理し活用していく知的資産経営が求められている。

○オープン・イノベーション
オープン・イノベーション（※）の促進ためには、事業者間で相互に営業秘密を開示しあうことが必要となるところ、その前提として実効的な営業秘密の管理が重要となる。

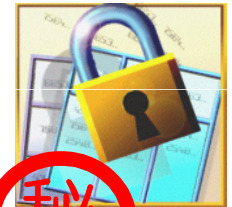
※「オープン・イノベーション」とは、企業等が情報を自社内でクローズにするのではなく、
企業間で相互に情報を開示し合うことにより、イノベーションを起こしていくことをいう。

○人的マネージメント
営業秘密管理の実効性を高めるためには、人的マネージメントの充実を図ることが重要である。

○営業秘密とは、不正競争防止法によって保護される、以下の３要件を全て満たす情報である。

➢ 秘密として管理されていること（秘密管理性）

①情報にアクセスできる者を制限すること　（アクセス制限）

②情報にアクセスした者にそれが秘密であると認識できること　（客観的認識可能性）

➢ 有用な営業上又は技術上の情報であること（有用性）

当該情報自体が客観的に事業活動に利用されていたり、利用されることによって、経費の節約、経営効率の改善等に役立つものであること。現実に利用されていなくても良い。

・設計図、製法、製造ノウハウ
・顧客名簿、仕入先リスト
・販売マニュアル

✕

・有害物質の垂れ流し、脱税等の反社会的な活動についての情報は、法が保護すべき正当な事業活動ではないため、有用性があるとはいえない。

➢ 公然と知られていないこと（非公知性）

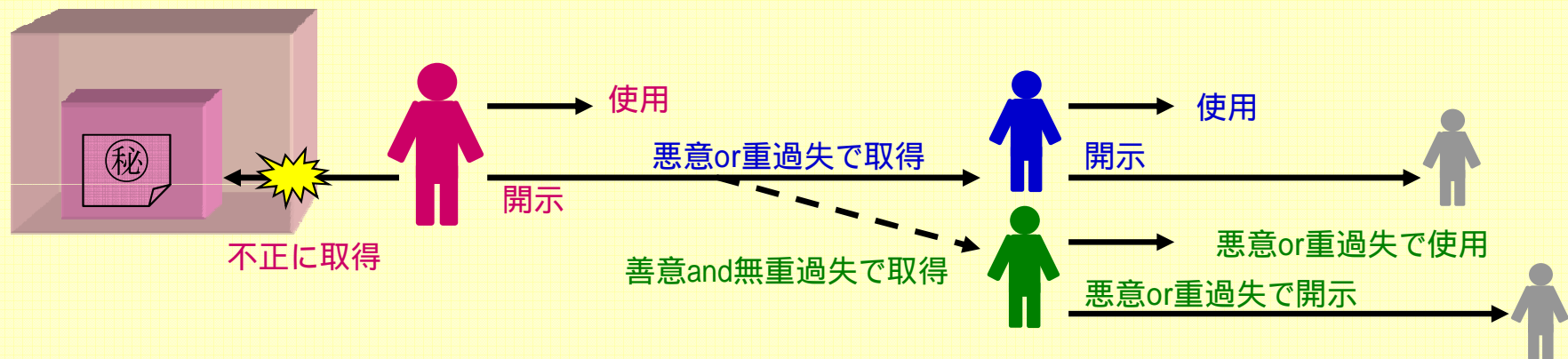
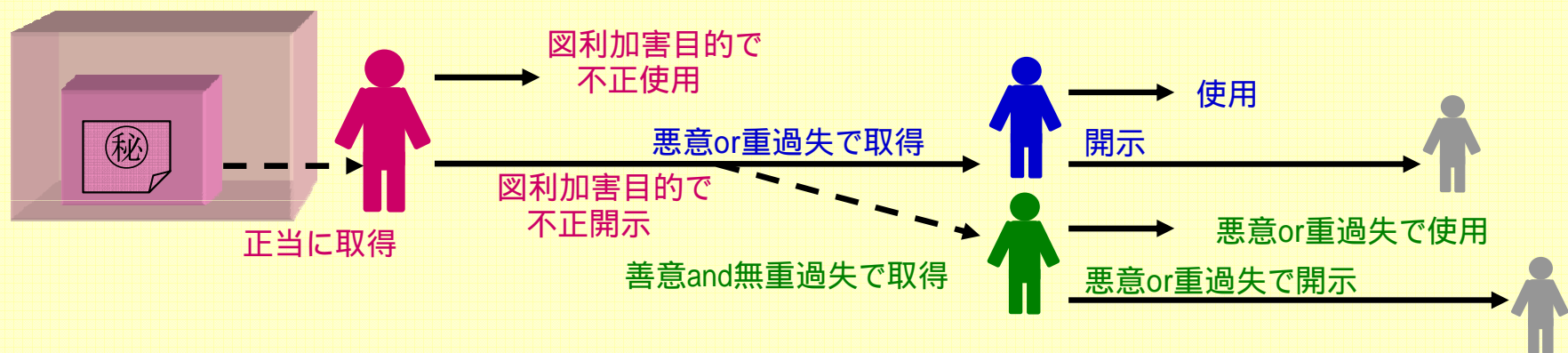
保有者の管理下以外では一般に入手できないこと。

○

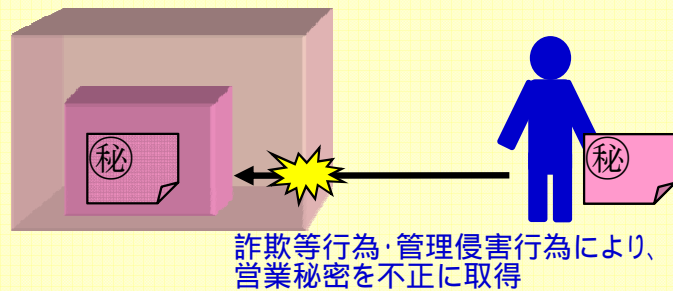
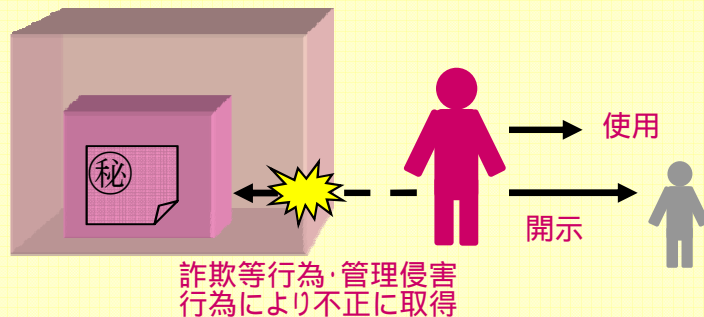
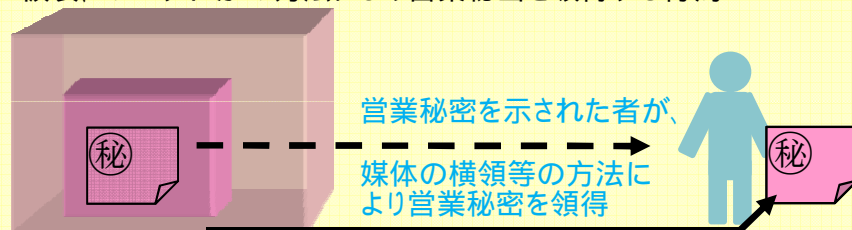
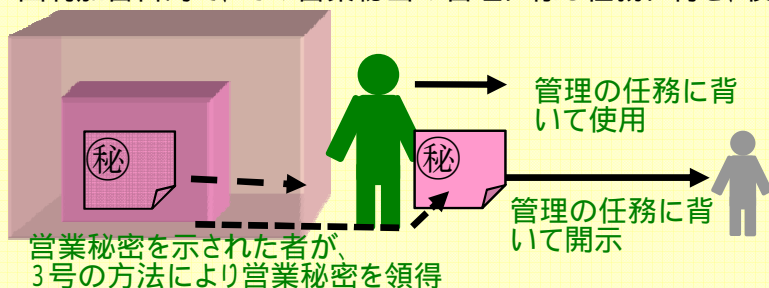
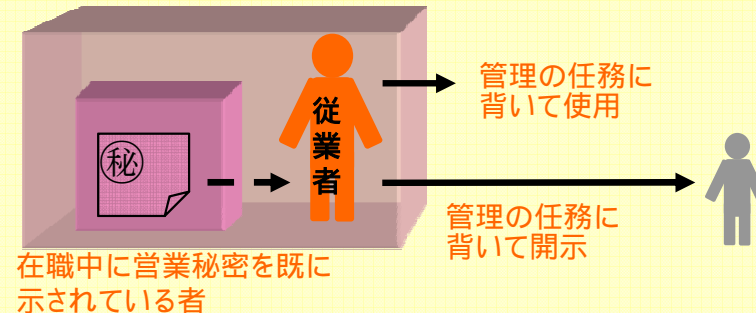
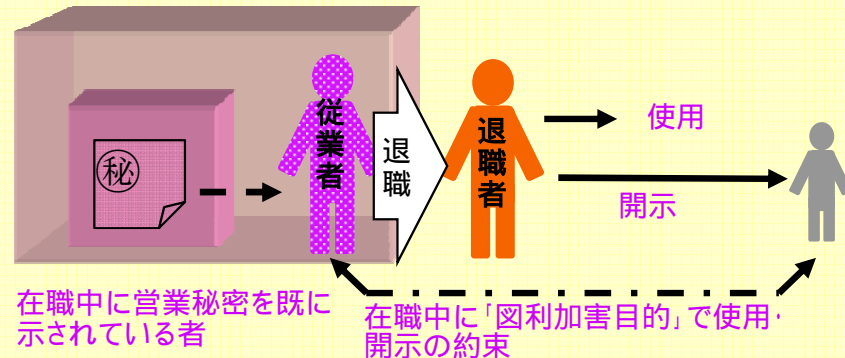
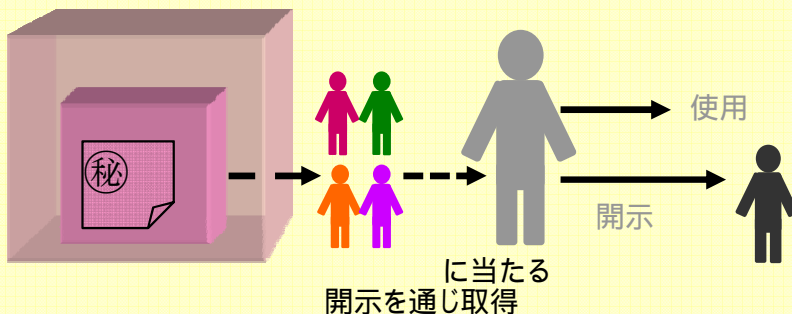
・第三者が偶然同じ情報を開発して保有していた場合でも、当該第三者も当該情報を秘密として管理していれば、非公知といえる。

✕

・刊行物等に記載された情報

○営業秘密侵害行為類型（第２条第１項第４号～９号）

※○囲いの数字は、不正競争防止法第２条第１項の各号の「不正競争」に該当することを意味する。
悪意or重過失＝当該行為があったことを知っている、あるいは重大な過失により知らないこと。
善意and無重過失＝当該行為があったことを、重大な過失なくして知らないこと。
図利加害目的＝不正に利益を上げたり、他人に損害を与える目的。

○営業秘密侵害罪の類型（第２１条第１項）

(1号) 図利加害目的で、詐欺等行為又は管理侵害行為によって、営業秘密を不正に取得する行為

(2号) 不正に取得した営業秘密を、図利加害目的で、使用又は開示する行為

(3号) 営業秘密を保有者から示された者が、図利加害目的で、その営業秘密の管理に係る任務に背き、(イ) 媒体等の横領、(ロ) 複製の作成、(ハ) 消去義務違反＋仮装、のいずれかの方法により営業秘密を領得する行為

(4号) 営業秘密を保有者から示された者が、第3号の方法によって領得した営業秘密を、図利加害目的で、その営業秘密の管理に係る任務に背き、使用又は開示する行為

(5号) 営業秘密を保有者から示された現職の役員又は従業者が、図利加害目的で、その営業秘密の管理に係る任務に背き、 営業秘密を使用又は開示する行為

(6号) 営業秘密を保有者から示された退職者が、図利加害目的で、在職中に、その営業秘密の管理に係る任務に背いて営業秘密の開示の申込みをし、又はその営業秘密の使用若しくは開示について請託を受け、退職後に使用又は開示する行為

(7号) 図利加害目的で、②、④～⑥の罪に当たる開示によって取得した営業秘密を、使用又は開示する行為

○平成２１年法改正後に、処罰対象となる行為類型と、
処罰対象とはならない行為類型とを、具体的に明示。

＜処罰対象となる行為の例＞

▸金銭を得る目的で、競業企業以外に営業秘密を不正に開示する行為
▸外国政府を利する目的で、営業秘密を外国政府関係者に不正に開示する行為
▸保有者に損害を加える目的で、持出しが禁止されたファイルを無断で外部に持ち出す行為

＜処罰対象とならない行為の例＞

▸公益の実現を図る目的で、企業の不正情報を内部告発する行為
▸労働者の正当な権利の実現を図る目的で、労使交渉により取得した保有者の営業秘密を、労働組合内部（上部団体等）に開示する行為
▸権限を有する上司の許可を受け、営業秘密をコピーしたり、営業秘密が記載された資料を外部に持ち出したりする行為

（参考）平成２１年法改正の背景

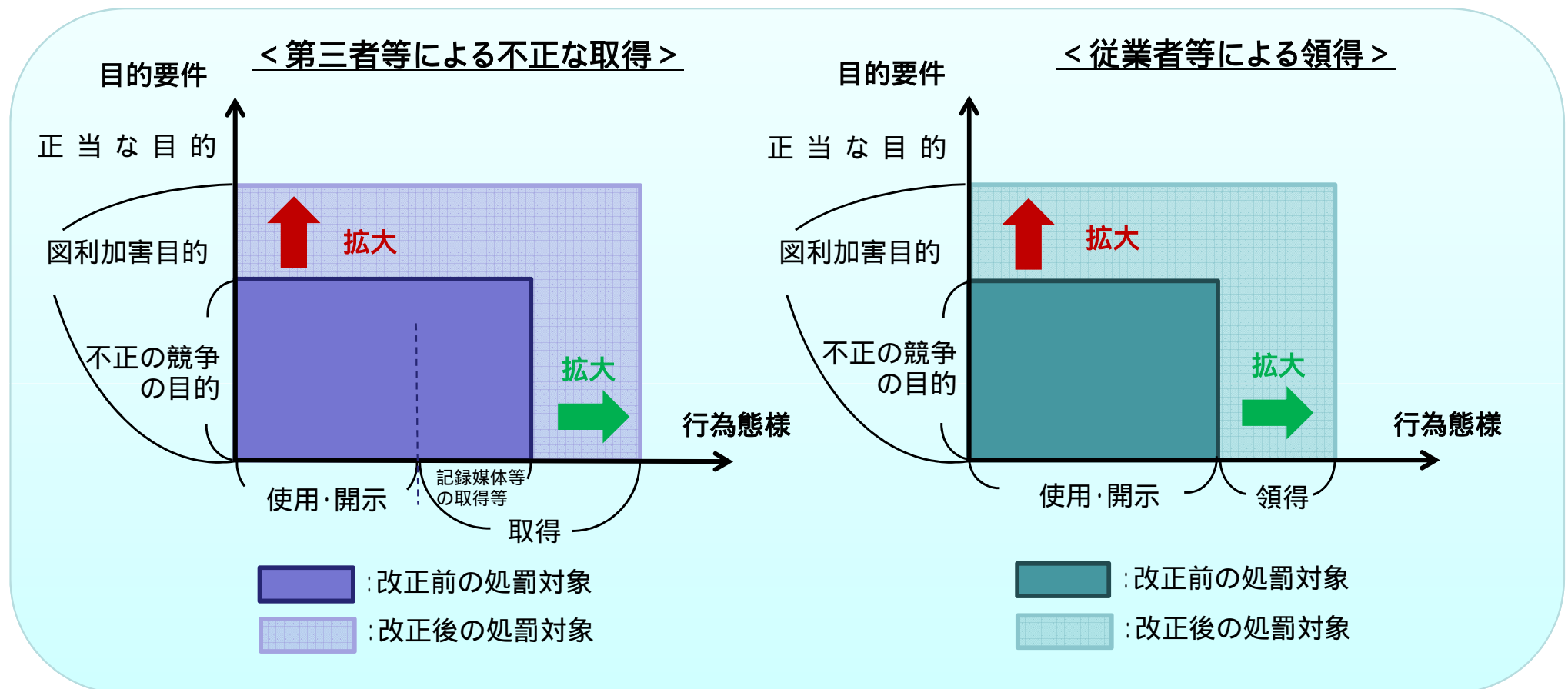
○近年、以下のような営業秘密に対する不正な侵害が多く発生し、法改正の必要性が指摘されていた。

＜従業員による機密情報の不正な持ち出し＞
ある企業に勤務する従業員が、当該企業が秘密として管理する図面データ等を貸与パソコンに大量にダウンロードし、無断で繰り返し自宅に持ち帰っていた。これを知った同社が同従業員に事情聴取を行ったところ、持ち出されたデータはどこにも残っておらず、貸与パソコンに記録媒体を装着した痕跡はあったが、不正にコピーがなされたと見られる私用パソコンが破壊されており、データの使用や外部への送信について確認することはできなかった。

＜外国政府によるデュアル･ユース技術の不正取得＞
元ロシア共和国在日大使館職員が、光学系機器メーカー従業員から、軍事転用されるおそれのある光通信の機密部品を不正に入手した。元大使館職員は警察の出頭要請に応じず帰国し、元従業員についても起訴猶予処分となった。

＜取引先企業によるノウハウの取り上げ＞
ある中小企業が、取引先である大手企業から、業務提携を前提として試作品を提供してほしい旨の申出を受け、試作品とその設計図面を提供したところ、取引先企業がその複製の作成をし、当該設計図面をもとに自社の製品として勝手に製品化をしてしまった。

（参考）平成２１年法改正の主な内容

①営業秘密侵害罪の目的要件の変更
②第三者等による営業秘密の不正な取得に対する刑事罰の対象範囲の拡大
③従業者等による営業秘密の領得自体への刑事罰の導入

第３章　営業秘密を保護するための管理の在り方

○ 営業秘密の管理に当たっては、「物理的管理」、「技術的管理」、「人的管理」等により、
－営業秘密を他の情報と区分し
－アクセスした者が秘密であると認識して取り扱うために必要な措置 及び
－権限のない者がアクセスできないような措置
を講じることが必要である。

○ また、これらの管理を適切に機能させるために「組織的管理」を行うことが重要である。

○合理的な管理がなされていることが重要である。

➢ 高度な管理方法

さらに高いセキュリティレベルを求める事業者は、営業秘密の漏えいリスクを最小化するための高度な管理手法を採用することも考えられる。

＜高度な管理方法の例＞
－プリンターで、デジタル透かし情報（廃棄期限や秘密表示など）を付加する。
－情報を外部に持ち出す際には、記録媒体に含まれる情報全体を暗号化する。
－コンピュータにアクセスする際に、生体認証などを利用する。
－理解度確認付きe-ラーニングなど全員の受講が確認できる教育プログラムを実施する。

➢ 一般的な管理方法

営業秘密として法律上の保護を受けるためには、必ずしも一律に高度な水準が要求されるものではない。

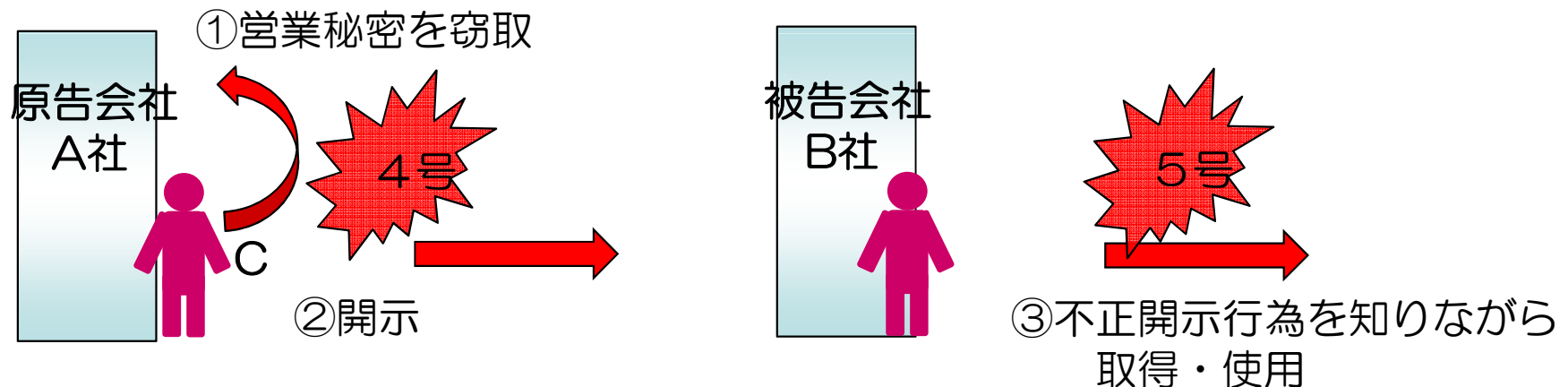
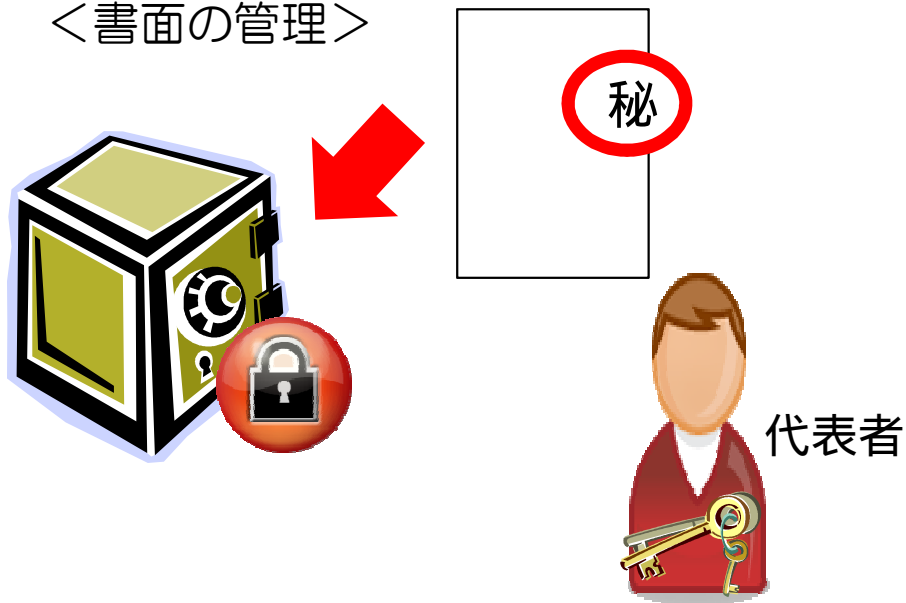
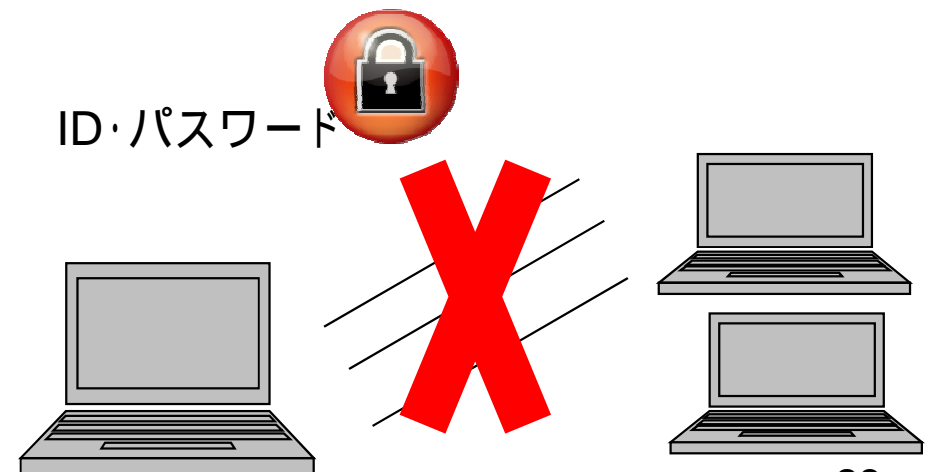
それぞれの事情を踏まえ、各種の管理方法を組み合わせて合理的な管理がされていれば足りる。

＜一般的な管理方法の例＞
－紙媒体の隅に、「厳秘」や「秘」などのスタンプを押したり、シールを貼り付ける。
－施錠可能な金庫、などに施錠して保管する。
－コンピュータの閲覧に関するパスワードやIDを設定する。
－定期的行われる朝礼などの際に、随時、営業秘密の取り扱いなどの注意喚起を行う。

（参考）具体的な裁判例：秘密管理性が肯定された例

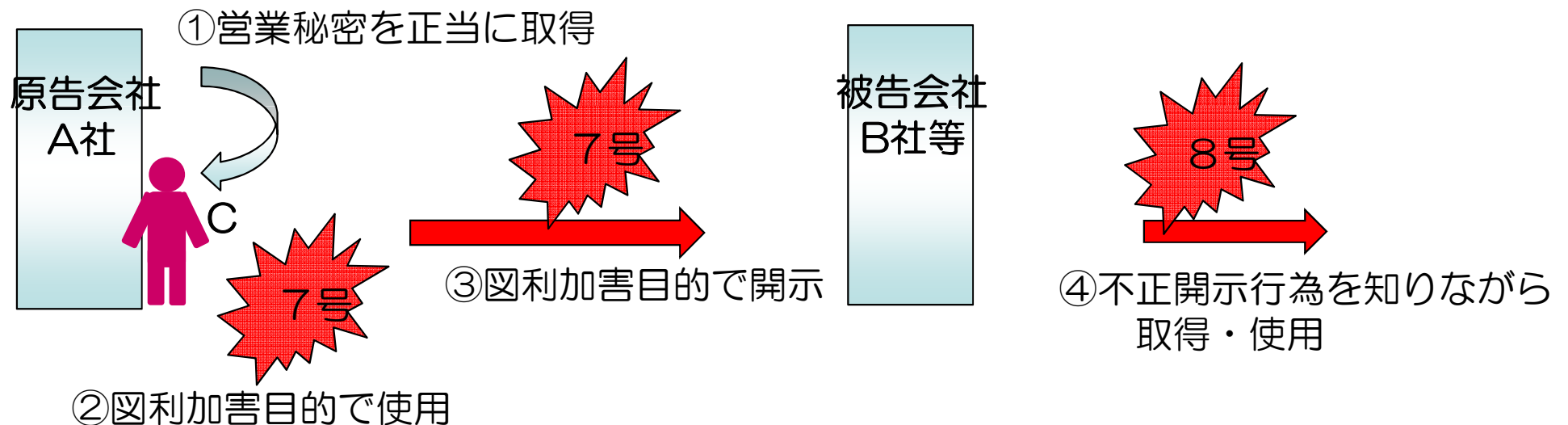
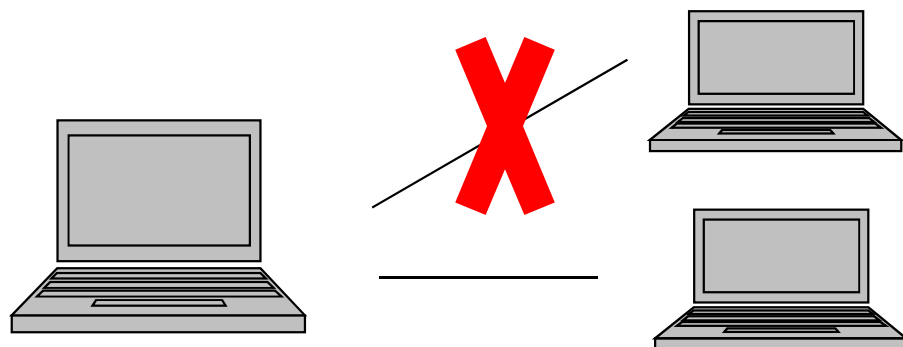
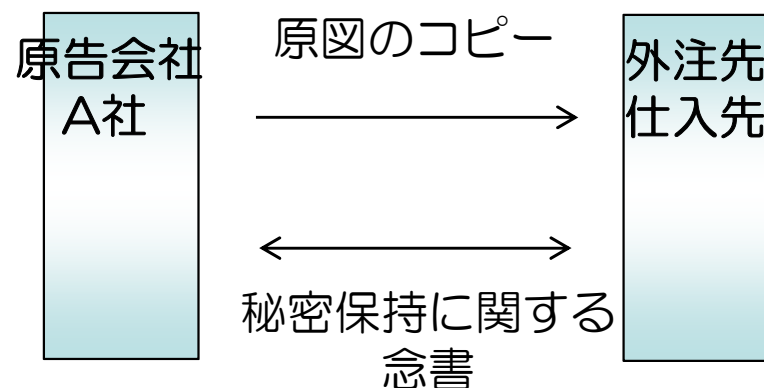
中国野菜輸入先・顧客名簿事件（東京地判平17.6.27）

＜争点となっている情報＞
輸入先目録・顧客目録

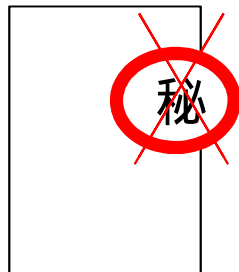
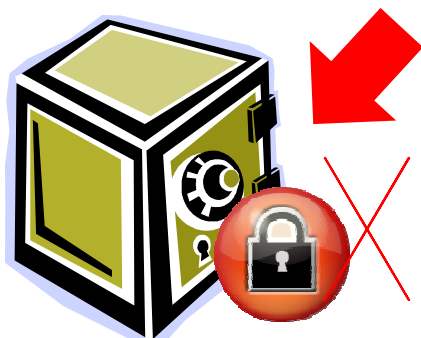
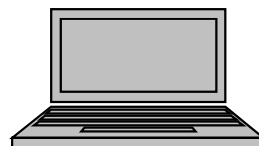
＜概要＞
原告会社（A社）と被告会社（B社）は中国野菜等を販売している。
A社の従業員であった被告（C）が営業秘密を窃取し、自身が取締役を務めるB社に開示した。
B社は、輸入先名簿を使用し、野菜生産者から利益率の高い野菜を輸入し、
さらに顧客名簿を使用し、A社の顧客の中でも売上高の多い顧客に対し、
A社よりも安い見積書を作成し販売した。

＜書面の管理＞
・「秘」と押印
・秘密書類保管用書庫に入れ施錠し、鍵を原告代表者（以下「代表者」という。）が管理
・閲覧には代表者の許可が必要
・閲覧しても原則謄写できない
＜電子データの管理＞
・代表者のパソコンに保管し、代表者のみ使用可能
・代表者のパソコンは他のパソコンやインターネットに接続していない
・代表者のパソコンを起動するには代表者のID・パスワードが必要
・本件情報が保存されているファイルにアクセスするにはID・パスワードが必要
＜人に対する管理＞
・秘密の範囲を具体化した誓約書を、本件情報にアクセスする従業員と締結
・就業規則に、秘密の範囲を具体的に記載し、秘密保持義務を負うことを明確化
・朝礼において、新聞等に掲載された営業秘密に関する事件を紹介

（参考）具体的な裁判例：秘密管理性が肯定された例

産業用ロボット営業秘密事件（名古屋地判平20.3.13 ）

<争点となっている情報>
設計図等（設計データ、表データ等）

<概要>
原告（A社）と被告会社２社（B社等）はロボットシステムを製造・販売している。
A社の従業員であった被告ら（C等）は、営業秘密を持ち出し、被告会社のロボットシステムを設計するため使用。
B社等は本設計に基づきシステムを製造・販売した。

<書面の管理>
・CADシステムで作成した設計原図は印刷し、手書設計図とともに、製造番号ごとにファイルで綴った上、鍵付きのキャビネットに保管（ただし未施錠）
・設計部門の従業員は設計図を持ち出す際、管理台帳に記載することは求められておらず、持ち出し後は机の引き出し等にて保管（机上へ放置やキャビネットへの未返却等も存在）
・設計部門以外の従業員は持ち出す際、管理台帳に記載することが平成１２年以降徹底
<電子データの管理>
・CADデータで作成した設計図等は、コンピュータサーバーに保管され、技術部門の端末からのみアクセス可能
・技術部門の従業員は、設計図等をコピー可能で、印刷後は設計原図と同様の取扱い
<取引先に対する管理>
・技術部門の従業員は、第三者に開示しないよう依頼せず外部に電子データを送付することがある
・設計原図のコピーを交付する外注先・仕入先との間で一部「秘密保持に関する念書」を取り交わしていた
・仕入先に対し、貸与等する図面等の管理方法を記載した｢文書管理要領｣を定めた
・設計図等と同様の組図が添付された取扱説明書を、秘密保持を申し入れずに交付したが、必要に応じ提供していたにすぎず、目的外使用を許諾していたとはいえない

（参考）具体的な裁判例：秘密管理性が否定された例

高周波電源装置情報事件（大阪地判平17.2.17）

<書面の管理>
・図面が保管されている設計室がある階には、「厳守業者立入禁止」等記載したボードがあったが、従業員は制限なく設計室に入ることができた
・開発設計部門の従業員は設計室からの持ち出しを認められており、他部門も閲覧は自由
・キャビネットは未施錠
・図面には秘密表示がされていない
<電子データの管理>
・図面は原則LANサーバーに保管されていたが、従業員のパソコンで保管されることもあった
・他部門の従業員はLANサーバーにアクセスできなかったが、設計開発部門のパソコンには図面の読み込みに必要なソフトが入っており、他部門の従業員は当該パソコンを立ち上げる際、所定のパスワードを入れることで閲覧できた
・図面をパソコンに保存することを制限したことはない
<人に対する管理>
・電子データの図面の取り扱いに格別の指示をしたことはない

参考資料１　営業秘密管理チェックシート

別添に掲載

○裁判例分析を踏まえた、秘密管理性について自己診断等ができるチェックシートである。

○活用方法としては以下が考えられる。

・自社診断ツール
・どの水準の管理体制を構築するか判断するための参照ツール
・情報毎に機密レベルを分ける場合に、どの機密レベルをどの管理水準で管理するか決める際の参照ツール

○得点を高めることにより、個別の事情の影響度を減少させ、秘密管理性が認められる可能性を高くすることができる。

営業秘密管理チェックシート（指定編）

No.	管理手順等	項　目	選択肢	内容	配点	加減事由	得点
以下の項目について、秘密情報ごとにチェックする							指定編
1	秘密指定	指定の有無・特定性	個別的・具体的	当該情報（それが保存・管理された書面、記録媒体、コンピュータを含む。以下同じ。）について、就業規則、誓約書、契約書、営業秘密管理規程その他の文書（以下「規程等」という。）によって従業者等（示された者）が秘密保持義務の対象となる情報として個別的・具体的に指定している。 例）「顧客情報（氏名、住所、性別、年齢等）」、「自社商品の原価情報」、特許のクレーム類似の特定など	50	口頭によって指定したにすぎない場合は30点	
			概括的等	当該情報について、規程等によって従業者等の秘密保持義務の対象となる情報として概括的に指定したり、営業秘密記録されるなどした媒体や保管先・保管施設等によって指定したりしている。 例）「○○製品の△△に関するデータ」、「他社との共同研究開発に関する秘密情報」、「ラボノート○○に記載された情報」、「○○データベースに記録された情報」、「○○工場の△△室において得られた情報」など	30	口頭によって指定したにすぎない場合は15点	
			包括的	当該情報について、規程等によって従業者等の秘密保持義務の対象となる情報として包括的に指定している。 例）「業務上の秘密」、「機密情報」など	10	口頭によって指定したにすぎない場合は5点	
			指定なし	当該情報について、秘密とすべきことを指定していない。	0		
2		組織的指定		営業秘密の指定・管理に関する規程又は管理基準を策定し、これに基づいた組織的な秘密指定プロセスによって、当該情報の秘密指定が行われている。	10		
3	アクセス権限の範囲指定	指定の有無	規程等で明確に指定（内部あり）	当該情報にアクセスできる者の範囲（役職、配属先、業務等）を規程等によって明確に指定している（規程等で責任者を明確にし、責任者が口頭又は書面によってアクセスできる者を明確にしている場合等も含む。）。 例）役員のみアクセスできる「極秘」、部配属者のみアクセスできる「部外秘」など	30		
			規程等で明確に指定（外部のみ）	当該情報に内部者以外がアクセスしてはならないこと（又は外部者によるアクセスを防ぐべきこと）を規程等によって明確に指定している。 例）「社外秘」など	10		
			事実上の内部制限	当該情報について、アクセスできる者の範囲を明確に指定した規程等はないが、配属先や担当業務によって事実上のアクセス制限を内部的に行っている。	10		
			明確な指定なし	当該情報にアクセスできる者の範囲を明確に指定していない。	0		
4		厳格な限定		当該情報にアクセスできる者について、役員・管理職以上といった、ごく一部の者に限定している。	10		

①50点以上の場合　→　チェックシート（管理編その１）へ（基礎点３０点、管理編７０点満点）
（秘密情報であると比較的容易に理解できるので、管理によって秘密としての実質が担保されていることが重要です。）
②50点未満の場合　→　チェックシート（管理編その２）へ（基礎点なし、管理編１００点満点）
（管理によって秘密としての実質が担保されるのみならず、それを通じて秘密情報であると理解できることも必要です。）

参考資料２　各種契約書等の参考例

○各企業における秘密管理において参考となる各種契約書等の参考例を示している。

○実際に本参考例を用いる際は、自社にとって参照することが適切かを十分検討し活用頂きたい。

（例）

・就業規則
・営業秘密管理規程
・入社時の秘密保持誓約書
・工場見学時の秘密保持誓約書
・取引基本契約書（製造請負契約）
・共同研究開発契約書

等

第１　就業規則（抄）

第○条（勤務規律）
１．社員は、職場の秩序を保持し、業務の正常な運営を守るため、職務を遂行するにあたり、次の各号に定める事項を守らなければならない。
○　会社の施設、設備、製品、材料、電子化情報等を大切に取り扱い保管するとともに、会社の許可なく私用に用いないこと。
○（以下略）
２．社員は、入退場に関し、次の各号に定める事項を守らなければならない。
○　会社の指示する手続を経て入退場すること。
○　警備員から所持品の検査を求められたときは、応じること。
○　日常携帯品以外の物品を携帯して入場しないこと。ただし、特に必要な場合は、会社の指示する手続をとること。
○　会社の許可なく、書類や社品を会社外に持ち出さないこと。
○　（以下略）
３．社員は、従業員証を常時携帯し、入場のとき又は求められたときは、直ちに提示しなければならない。

第○条（遵守事項）
社員は、次の各号に定める事項を守らなければならない。
○　会社の内外を問わず、在籍中又は退職若しくは解雇により社員資格を失った後も、会社の機密事項を、不正に開示したり、不正に使用したりしないこと。
○　会社の許可なく、在籍中又は退職若しくは解雇により社員資格を失った後も、前項の事項を使用して競業的行為を行わないこと。
○　会社の諸規則に違反する出版若しくは講演などを行わないこと。
○　会社の許可なく、立入禁止区域に立ち入り、又は業務外の事由で自己の職場以外に立ち入り、若しくは会社の施設・敷地を利用しないこと。
○　業務上知った会社の機密事項を使用し、在籍中又は退職後においてその公表前に直接若しくは間接的に関連株式の売買を行わないこと。
○　（以下略）

第○条（入場制限・退場命令）
社員が次の各号の一に該当すると会社が認めた場合は、入場させず、又は退場させることがある。
○　入退場手続を行わないとき。
○　従業員証を所持していないとき。
○　警備員による所持品の検査に応じないとき。
○　業務外の事由で入場しようとするとき又は終業後退場しようとしないとき。
○　（以下略）

参考資料３　我が国における情報管理に関する各種ガイドライン等

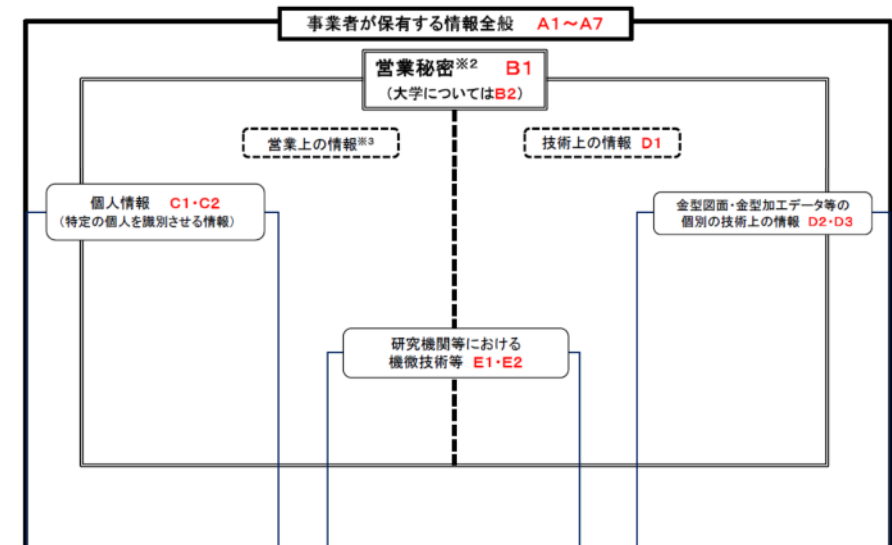
○本図表は、公的機関等により提示されている各種ガイドライン等とその対象となる情報との対応関係を概観できる図表である。

○例えば顧客情報は、営業秘密という観点からの管理と個人情報保護法からの管理が求められる場合があるなど、同一の情報でも異なる管理を要請される場合がある。

○本図表を用いることで、効率的な管理の在り方を整理・把握することが期待される。

我が国における情報管理に関するガイドライン等一覧

		公表年	文書提示機関	目的・特徴	対象とする情報の種類	産業の特定	遵守レベル	求められる措置	文書内で示された管理の水準※		
									基本方針	対策基準	具体的取組
A　組織の情報全般を扱うもの											
1	情報セキュリティガバナンス導入ガイダンス ※情報セキュリティに関する文書は、目的・対象に合わせて経済産業省等より複数発行されている。	2009	経済産業省	組織が効率的に情報セキュリティマネジメント体制を構築し、適切な管理策の整備と運用を行えるよう情報セキュリティマネジメントの基本的な枠組みと具体的な管理項目を規定したもの。	企業が保有する情報全般	全産業	遵守義務はないが、組織体として情報セキュリティ管理体制が整備されていると外部から認識されるためにはおさえておくべきである。	JISQ27001,JISQ27002に準拠した形で網羅的かつ具体的に組織が備えるべき管理体制を列挙している。			
2	アウトソーシングに関する情報セキュリティ対策ガイダンス	2009	経済産業省	組織がアウトソーシングを検討、実施する際に対応を検討すべきリスクの提示及びアウトソーシング先に求める対策等、事前検討事項、及びその実施方策等を示したもの。	企業が保有する情報全般	全産業	遵守義務はない。	組織がアウトソーシングを検討する上での具体的に検討すべき事項について列挙している。			
3	JISQ27001,JISQ27002 (ISO/IEC27001,ISO/IEC27002)	2006	JIS（ISO/IEC）（国際標準規格）	組織が保有する情報資産についてのリスクを分析し、それをマネジメントする手順を示すもの。	企業が保有する情報全般	全産業（認定は部門ごとでも可能）	この規格に基づき、ISMS認証を希望する場合は一定の水準を満たす管理体制を構築する必要がある。	情報セキュリティマネジメントシステムを構築し運用するために必要な具体策を列挙している			
4	職場外のパソコンで仕事をする際のセキュリティガイドライン	2006	総務省	職場外でパソコンを使用する際に想定される危険性を前提に、モデルケースとしての対策等を例示するもの。	企業が保有する情報全般（パソコンで扱う情報）	職場外で従業員がパソコンを使って業務を行う企業	遵守義務はない。	技術的・組織的・人的管理方針を概括的に示しているが、職場外でのPC使用時の留意点を示しているため、物理的管理に関する記述は少ない。			

（相互に参照）

参考資料４　導入手順例

○管理体制を構築するための具体的な導入手順を紹介している。

①自社の強みとなる情報資産を把握する。
（営業秘密として管理する情報資産の把握）

Step１
技術やノウハウ、ブランド力等の自社の強みとなる知的資産を把握する。

⇒

Step２
製造プロセス、販売マニュアル、仕入先等、知的資産を構成する具体的な情報を把握する。

⇒

Step３
把握した具体的な情報の中から、営業秘密として管理したいと考える情報を選択する。

Step1	Step2	Step3
個性的な製品等を完成させるための技術やノウハウ	・製造プロセス・段取りに関する情報 ・研究開発情報（技術開発・試験記録等） ・製造協力先・下請事業者の情報	営業秘密として管理したいと考える情報を選択
中長期的な取引関係等に基づく信頼に裏打ちされた製品等や、事業者のブランド力	・仕入先・販売先・品目・数量・価格情報等 ・販売マニュアル、サービスマニュアル等 ・販売協力先（代理店・ＦＣ等）情報 ・製品・商品・サービスに対する利益額（率）	
顧客のニーズに応える製品等を提供する営業力	・顧客から受け取る各種資料及び情報 ・顧客との各種契約情報及び契約内容	
高い技術を有する従業者	・技術者教育・育成に関する情報 （教育プログラム・資料等）	

参考資料４　導入手順例

②チェックシートを用いて現在の管理水準を認識する。

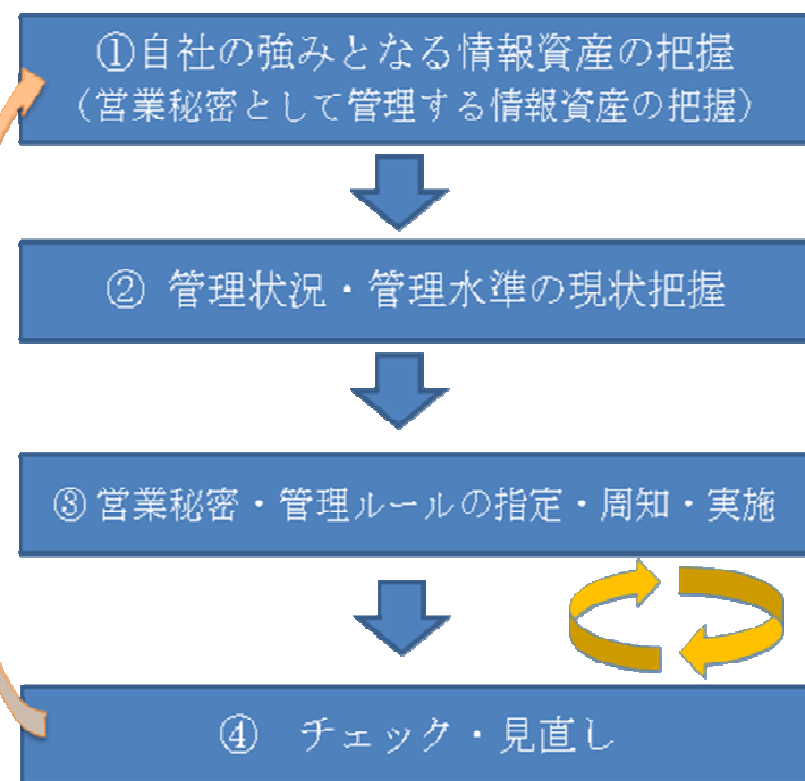
③営業秘密の管理ルールを決め、周知、実施する。

事業者の規模、業種、営業秘密として管理する情報量、取扱状況を踏まえ、

Step1　チェックシートを用いて目標とする管理水準を検討する。
Step2　管理方法を選択する。
Step3　選択した管理方法を書面等用いて周知する。

④管理ルールが適切に行われているかチェック・見直しをする。

○構築した管理ルールが実効性を欠く事態に陥っている場合には、営業秘密として認められないおそれがあるため、管理状況をチェックすることが望ましい。
○チェック方法としては、規模等に応じて、例えば社長が日常的に目を配る、監査を実施する、などを行うことが考えられる。
○実効的な管理が行われていない場合には、要因に応じて対応策を実施する必要がある。

＜具体的な導入手順の流れ＞

営業秘密管理チェックシート

営業秘密管理指針に関するご質問はこちらまで
経済産業省　経済産業政策局　知的財産政策室
〒１００－８９０１　東京都千代田区霞が関1丁目3番1号
ＴＥＬ：０３－３５０１－３７５２　ＦＡＸ：０３－３５０１－３５８０
Ｅ－mail：chitekizaisan@meti.go.jp

営業秘密管理指針（改訂版）概説

発　行　　２０１０年　9月　１日
編　著　　経済産業省知的財産政策室